

明 細 書

フレーム中継装置

技術分野

本発明は、フレーム中継装置に関し、特に、アドレスのなりすましによる、他のサーバまたは端末に対する攻撃を防止するフレーム中継装置に関する。

背景技術

従来から、個々のネットワーク接続機器に付与されるIP（Internet Protocol）アドレス、あるいは上記ネットワーク接続機器に固有なMAC（Media Access Control）アドレスを他の接続機器のものと偽る、いわゆるアドレスのなりすましの問題があった。このようなアドレスのなりすましのうち、IPアドレスのなりすましは、例えば、送信元IPアドレスを適当な他人のものに書き換えることによって容易に行うことができる。また、MACアドレスのなりすましは、IPアドレスのなりすましと比較すると難しいものの、他人が用いるMACアドレスになりすますことは可能である。そして、アドレスをなりすました後で、インターネットに接続している各種サーバや端末に対してDoS（Denial of Services：サービス拒否）攻撃等のネットワークからの攻撃、あるいはネットワークからの侵入が行われた場合には、IPアドレスやMACアドレスが本来のアドレスとは異なるため、その攻撃元あるいは侵入元を特定するのは困難であった。

通常は、アドレスのなりすましを防止するために、所定の条件によってフレームを選別して、中継が必要なフレームのみを中継する、いわゆるフィルタリング処理を行う。このようなフィルタリング処理の機能は、ファイアウォール、負荷分散装置、あるいはルータやレイヤ3スイッチ等の中継装置に実装されている。

ところで、上記のようなフレームの中継装置に実装されているフィルタリング機能は、装置本来のフレームの中継性能を維持するために、フレームのヘッダについている情報（例えばIPアドレス等）がフィルタリングの対象であるか否かを見ることによって中継するフレームであるか否かを選別していた。このため、なりすましによって侵入元や攻撃元のアドレスを度々変更された場合には、その変更に係るア

ドレスがフィルタリング対象を判定するアドレステーブルに無ければ、このようなフレームはフィルタリングされないもので、なりすましを防止することができない。一方、中継装置が受け付ける或るサービスに係る全てのフレームをそのアドレスの如何に拘わらずフィルタリング対象にすると、当該中継装置で当該サービスに係るフレームは全て遮断されてしまうので、当該中継装置を経由してサーバにアクセスする全ての端末が当該サーバの提供するサービスを受けることができなくなる可能性があった。

また、ファイアウォールあるいは負荷分散装置では、ネットワークを経由した攻撃を検知した段階でその攻撃の送信元アドレスからのフレームを中継しないようにすることは可能であった。しかしながら、なりすましのアドレスが再三にわたって変更された上で攻撃を継続するなどされた場合には、送信されたフレームが攻撃のためのフレームか否かの判別が困難であった。

さらに、通常のファイアウォールは、インターネットなどの外部のネットワークに接続する箇所に設置される。また、負荷分散装置は、負荷分散対象となるサーバに直結する箇所に設置される。この場合、ファイアウォールあるいは負荷分散装置に至るまでの経路に当たるネットワークが攻撃用の多量のフレームによって輻輳を起こしてしまうため他のフレームが伝送されないという問題があった。

このような問題を解決するには、全ての端末付近にファイアウォールあるいは負荷分散装置を設置し、端末の直近でその攻撃フレームを排除する必要がある。しかしながら、設置の費用及び作業を考慮すると、全ての端末付近にこのような装置を設置することは困難であった。

なお、このようなIPアドレスやMACアドレスといったアドレスのなりすましによる攻撃防止に関する技術として、無線通信における端末移動によるアドレス変更において、アクチベーション（正規のライセンスを持っていることを証明すること）を行うことでなりすましを防止する技術（例えば、特許文献1参照。）が開示されている。

特許文献1

特表2003-518821号公報

本発明は上述したような従来の技術の問題点に鑑みてなされたものである。すな

わち、本発明の課題は、ルータ、レイヤ3スイッチ、レイヤ2スイッチ(スイッチングHUB)のようなフレーム中継装置において、アドレスのなりすましによるフレームの中継を防止できるような技術を提供することにある。

発明の開示

本発明は前記課題を解決するために、以下の手段を採用した。

すなわち、本発明は、フレーム中継装置であり、自装置でのフレームの中継処理で使用するMACアドレスとIPアドレスとの組を含むエントリが登録されるテーブルと、受信されたフレーム中の送信元MACアドレス及び送信元IPアドレスで前記テーブルを検索し、この送信元アドレスの組がレイヤ3での中継対象として登録されているか否かを判定する判定手段と、前記送信元アドレスの組が中継対象として登録されていると判定されたフレームのみを対象としてレイヤ3の中継処理を行うレイヤ3中継処理手段とを備える。

本発明のフレーム中継装置によると、中継対象がMACアドレスとIPアドレスとの組を含むエントリが登録されるテーブルに基づいて、受信したフレームに対する中継対象(ルーティング対象)であるか否かの判別処理を行う。そして、本発明のフレーム中継装置では、ルーティング対象のフレームについて中継処理(ルーティング処理)を行う。テーブルには、正規に端末や中継装置に割り当てられたMACアドレス及びIPアドレスの組が登録され、MACアドレスやIPアドレスをなりすました不正なアドレスの組は登録されないように構成される。従って、本発明によれば、受信したフレームのうち、なりすましなどの中継が許可されていないフレームの中継を防ぐことができる。

また、本発明は、前記フレームの送信元アドレスの組が前記テーブルに登録されていなかった場合に、この送信元アドレスの組が正常か否かを問い合わせるための問い合わせフレームを送信し、この問い合わせフレームに対する応答フレームが前記問い合わせフレームを送信してから所定期間内に到着し且つこの応答フレーム中の情報が前記送信元アドレスの組が正常であることを示すという条件を満たすか否かを判定し、前記条件を満たす送信元アドレスの組を含むエントリを前記テーブルに登録し、前記条件を満たさない送信元アドレスの組を前記テブ

ルへの登録対象から除外する中継対象登録手段を備えるように構成することが好ましい。

本発明のフレーム中継装置によると、受信したフレームを前記テーブルに登録する(ルーティングを許可する登録を行う)前に、問い合わせフレームを送信する。そして、フレーム中継装置では、問い合わせフレームに対する応答が正しいことを判断した後に、この送信元アドレスの組み合わせが正しいものとして受信したフレームの送信元アドレスの組を含むエントリの登録を行う。このようにすれば、フレーム受信時に、例えば、アドレスをなりすましたフレームの送信元アドレスの組を中継対象として登録することを防止できる。

また、本発明の前記中継対象登録手段は、前記問い合わせフレームとして前記フレームの送信元IPアドレスに対応するMACアドレスを問い合わせるためのARP (Address Resolution Protocol) 要求フレームを送信し、前記応答フレームとしてARP応答フレームを受信し、このARP応答フレーム中の問い合わせ先のMACアドレスが前記フレームの送信元MACアドレスと一致する場合に、前記送信元アドレスの組み合わせが正常であると判定してもよい。

このようにすれば、本発明の問い合わせフレームとして、既存のARP要求フレームを用いるため、新たな問い合わせフレームを生成することなく、本発明の処理を実行することができる。

さらに、本発明の前記中継対象登録手段は、前記問い合わせフレームとして前記フレームの送信元MACアドレス及び送信元IPアドレスをそれぞれ宛先MACアドレス及び宛先IPアドレスとするping (Packet INternet Groper) フレームを送信し、前記応答フレームとしてpingリプライフレームを受信し、このpingリプライフレームの送信元MACアドレス及び送信元IPアドレスが前記フレームの送信元MACアドレス及び送信元IPアドレスにそれぞれ一致する場合に、前記送信元アドレスの組み合わせが正常であると判定してもよい。

このようにすれば、本発明の問い合わせフレームとして、既存のpingフレームを用いるため、新たな問い合わせフレームを生成することなく、本発明の処理を実行することができる。

また、本発明の前記中継対象登録手段は、前記フレームの送信元IPアドレス

と同一のIPアドレスを含むエントリが既に前記テーブルに登録されている場合には、前記応答フレームに係る条件が満されるか否かに拘わらず、前記フレームの送信元アドレスの組を前記テーブルへの登録対象から除外してもよい。

このようにすれば、MACアドレスをなりすましたフレームが中継対象としてテーブルに登録されるのを防止することができる。

また、本発明の前記中継対象登録手段は、前記フレームの送信元MACアドレスと同一のMACアドレスを含むエントリが既に前記テーブルに登録されている場合には、前記応答フレームに係る条件が満されるか否かに拘わらず、前記フレームの送信元アドレスの組を前記テーブルへの登録対象から除外してもよい。

このようにすれば、例えば、IPアドレスをなりすましたフレームが中継対象として登録されることを防止することができる。

また、本発明は、前記テーブルに対してMACアドレスが同一でありIPアドレスが異なるエントリを登録可能な数が予め規定されており、前記中継対象登録手段は、前記フレームの送信元MACアドレスと同一のMACアドレスを含む前記登録可能数以上のエントリが既に前記テーブルに登録されているときには、前記応答フレームに係る条件が満されるか否かに拘わらず、前記フレームの送信元アドレスの組を前記テーブルへの登録対象から除外するように構成してもよい。

本発明によると、中継対象として許可するフレームの送信元アドレスの組をテーブルに登録する前に、このフレームの送信元MACアドレスと同一のMACアドレスに対応する登録済のIPアドレスの数を取得する。そして、このIPアドレスの登録数が、予め定められた同一MACアドレスに対するIPアドレスの登録可能数以上であれば登録処理を行わない。従って、本発明によれば、登録可能数を複数に設定することで、同一の端末がIPアドレスを変更した場合におけるMACアドレス及びIPアドレスの組をテーブルに登録することを許容する。一方で、登録可能数以上のアドレスの登録を防止して、なりすましのアドレスの登録を防止することができる。

また、本発明は、前記テーブルが、MACアドレスとこのMACアドレスに対応する宛先ポート番号とを含むエントリを格納し、フレームのレイヤ2での中継において宛先ポートを割り出すために参照されるMACアドレステーブルの各エ

ントリに、MACアドレスに対応するIPアドレスのフィールドと、中継対象か否かを示す情報を格納するフィールドとを設けることによって構成され、自装置で受信されるフレームのレイヤ2の中継処理を前記テーブルを参照して行うレイヤ2中継処理手段と、前記テーブルから一定時間使用されなかったエントリを削除する削除手段とをさらに備えるように構成してもよい。

本発明によると、中継対象とするか否かを判断するためのテーブルを、通常のレイヤ2の中継装置で用いるMACアドレステーブルに組み込むことができる。従って、本発明によれば、レイヤ2の中継処理とルーティング対象のチェックを1つのテーブルで行うことができる。また、MACアドレステーブルに対するエージング処理の利用による自動エントリ削除を実現することができる。

また、本発明は、前記フレームの送信元アドレスの組を含むエントリを前記テーブルに登録する際に、この送信元アドレスの組を構成するMACアドレスと同一のMACアドレスを含む他のエントリが既に前記テーブルに登録されている場合には、前記判定手段による処理において当該エントリが前記他のエントリよりも先に検索される状態で当該エントリを登録してもよい。

本発明によると、所定時間経過後のエントリを削除する、いわゆるエージング処理によって、古いIPアドレスを持つエントリが自動で削除される。従って、本発明によれば、使用されていないIPアドレスを含むエントリを、テーブルから確実に削除することができる。

また、本発明は、自装置が有するポート毎に前記判定手段及び前記中継対象登録手段による処理を行うか否かを設定可能に構成されてもよい。

このようにすれば、個々のポートに接続する接続装置やネットワークの状況に応じて、本発明の処理を実行するか否かを設定することができる。

また、本発明は、自装置が有するポート毎に受信可能なMACアドレスを一つだけ登録可能なテーブルと、各ポートで受信されたフレームに対し、このフレームの送信元MACアドレス及び受信ポート番号の組と同一のMACアドレス及びポート番号の組が前記テーブルに登録されているか否かを判定する判定手段と、前記送信元MACアドレス及び受信ポート番号の組が登録されていると判定されたフレームのみを対象としてレイヤ2の中継処理を行う中継手段とを含むフレー

ム中継装置として特定することができる。

本発明によると、中継対象を定義したテーブルには、中継装置の持つポート毎に一つのMACアドレスが用意される。また、本発明では、受信したフレームの送信元MACアドレスと対応するMACアドレス及び受信ポート番号の組を、テーブルから検索して中継処理を行う。従って、本発明によれば、レイヤ2中継処理において、MACアドレスがなりすまされたフレームの中継を防ぐことができる。

また、本発明は、前記フレームの送信元MACアドレスが、前記テーブルに登録されていない場合に、この送信元MACアドレス及び受信ポート番号の組が有効であるか否かを判定し、有効なフレームの送信元MACアドレス及び受信ポート番号の組を前記テーブルに登録する、MACアドレス学習部をさらに含んでもよい。

このようにすれば、MACアドレス学習機能を利用して、有効と認められるMACアドレス及びポート番号の組をテーブルに登録することができる。ここで、MACアドレスがなりすまされた送信元アドレス及び受信ポート番号の組が無効とされることで、当該組が登録されるのを防止することができる。

また、本発明の前記MACアドレス学習部は、前記ポートがフレームを受信可能な状態となってから、最初に受信したフレームの送信元MACアドレス及び受信ポート番号の組を、前記有効な組としてテーブルに登録するのが好ましい。ここで、当該状態とは、中継装置が起動したときに、この中継装置の全てのポートについて生じる。あるいは、中継装置起動中において、あるポートに対するリンクが切れ、その後、このポートについてリンクが接続されたときに生じる。

本発明によると、MACアドレス学習部が、ポートから最初に受信したフレームの送信元MACアドレス及び受信ポート番号の組を有効な組として登録し、このフレームの中継を行うためにテーブルに登録する。従って、本発明によれば、有効な組をテーブルに登録した後に受信したなりすましフレームの中継を防止することができる。

また、本発明の前記MACアドレス学習部は、送信元MACアドレス及び受信ポート番号の組が有効であるか否かの判断を行うか否かをポート毎に設定可能で

あってもよい。

このようにすれば、個々のポートに接続される装置やネットワークの状況に応じて、本発明の処理を実行するか否かを設定することができる。

なお、本発明は、コンピュータに本発明に係る手段の何れかの機能を実現させるプログラムとして特定することができる。また、本発明は、そのようなプログラムが記録されたコンピュータが読み取り可能な記憶媒体として特定することができる。さらに、本発明は、フレーム中継装置に搭載される、レイヤ3やレイヤ2の中継の判定処理を行う装置として特定することができる。

図面の簡単な説明

図1は、第1の実施の形態に係るフレーム中継装置の構成を示すブロック図であり、

図2は、従来のレイヤ2スイッチにおけるレイヤ2中継処理を示すフローチャート及びMACアドレステーブルの一例であり、

図3は、第1の実施の形態に係るMACアドレステーブルの一例であり、

図4は、フレーム中継装置のレイヤ2中継処理部によるレイヤ2中継処理を示すフローチャートの一例であり、

図5は、従来のレイヤ2スイッチにおけるレイヤ2アドレス学習処理を説明するフローチャートの一例であり、

図6は、フレーム中継装置のレイヤ2アドレス学習処理部による、レイヤ2アドレス学習処理を説明するフローチャートの一例であり、

図7は、第2の実施の形態に係るフレーム中継装置の構成を示すブロック図であり、

図8は、ルーティング対象チェック部による、ルーティング前処理について説明するフローチャートの一例であり、

図9は、ルーティング対象登録処理部による、ルーティング対象登録処理を説明するフローチャートの一例である。

図10は、ルーティング対象登録処理部による、ルーティング対象登録処理を説明するフローチャートの一例である。

発明を実施するための最良の形態

以下、図面を参照して、本発明のフレーム中継装置の一実施の形態を説明する。本発明のフレーム中継装置は、スイッチングハブ、レイヤ2スイッチ、ルータ、レイヤ3スイッチ、L2及びL3の中継機能を併せ持つ装置(L2/L3スイッチ)等に適用できる。

本実施の形態は、レイヤ2スイッチやスイッチングHUBに適用可能な本発明に係るフレーム中継装置の一例を、第1の実施の形態として説明する。また、レイヤ3スイッチ、ルータ、L2/L3スイッチに適用可能な本発明に係るフレーム中継装置の一例を、第2の実施の形態として説明する。

〈第1の実施の形態〉

図1は、第1の実施の形態に係るフレーム中継装置の構成を示すブロック図である。フレーム中継装置10は、レイヤ2中継処理部11、MACアドレステーブル12、レイヤ2アドレス学習処理部13、許容MACアドレステーブル14を備える。

なお、フレーム中継装置10の機能ブロックのうち、レイヤ2中継処理部11は、本発明の判定手段及び中継手段として機能する。また、レイヤ2アドレス学習処理部13は、本発明の判定手段、登録手段、及び切り替え手段として機能する。

レイヤ2中継処理部11は、複数(例えばn個)のポート15のそれぞれで受信されるフレームを受け取る。レイヤ2中継処理部11は、MACアドレステーブル12を参照して、各フレームに対する後述のレイヤ2中継処理を実行する。このレイヤ2中継処理によってフレームを中継するあて先が定められる。レイヤ2中継処理後、レイヤ2中継処理部11は、フレームをレイヤ2アドレス学習処理部13に送信する。

なお、レイヤ2中継処理部11は、MACアドレステーブル12から、古い検索対象のフレームの情報(エントリ)を削除するために、いわゆるエージング処理(時間経過による処理)を行う。エージング処理では、エントリが登録されてから所定の時間(例えば、IPv4であれば通常30秒)が経過するまでの間に、そのエントリに対するアクセスが無ければ、そのエントリが削除される。

図3は、フレーム中継装置10に搭載されるMACアドレステーブル12の一例である。MACアドレステーブル12には、フレーム中継装置10の中継対象であるMACアドレスが格納されている。そして、MACアドレステーブル12には、MACアドレスにそれぞれ対応するIPアドレス、宛先ポート、ルーティング対象の有無が格納されている。

レイヤ2アドレス学習処理部13は、後述の許容MACアドレステーブル14を用いて、入力されたフレームに対する後述のレイヤ2アドレス学習処理を実行する。レイヤ2アドレス学習処理後、レイヤ2アドレス学習処理部13は、レイヤ2中継処理に基づいた宛先に対応した出力先のポート15へフレームを出力し、フレームは当該ポート15から送出される。

許容MACアドレステーブル14は、レイヤ2アドレス学習処理部13による処理のために新規に用意されるテーブルである。また、許容MACアドレステーブル14は、なりすましたMACアドレスでの学習処理を防ぐために用意される。図6に、許容MACアドレステーブル14の一例を示す。本テーブル14は、フレーム中継装置10の持つ個々のポート15に対応するエントリを持つ。そして、個々のエントリは、個々のポート15のポート番号に対応する、MACアドレスの有効/無効を示す値を格納するフィールドと、そのポート番号で受信して良いMACアドレスを格納するフィールドとを持つ。各エントリにおいて、MACアドレスの有効/無効を示す値は、MACアドレスのフィールドに設定されたMACアドレスが有効であるか否かを示す。

上述したフレーム中継装置10に係る構成のうち、レイヤ2中継処理部11及びレイヤ2アドレス学習処理部13は、従来のフレーム中継装置における中継機能及び学習機能のそれぞれの処理内容に改変を加えることで実現することができる。

〈レイヤ2中継処理〉

次に、フレーム中継装置10で実行されるレイヤ2中継処理について説明する。

図2は、本発明との比較のための、従来のレイヤ2スイッチにおけるレイヤ2中継処理を示すフローチャート及びMACアドレステーブルの一例である。図2に示す処理では、レイヤ2スイッチは、受信されたフレームの宛先MACアドレ

スを抽出して、レイヤ2スイッチ内のMACアドレステーブルからこの宛先MACアドレスに対応するポートを検索する。MACアドレステーブルには、MACアドレスと、これに対応する宛先のポートの識別情報が格納されている。レイヤ2スイッチは、MACアドレステーブルから宛先MACアドレスに対応する宛先ポートが検索できた(送信元MACアドレスと同じMACアドレスを持つエントリがヒットした)場合には、当該フレームを当該宛先ポートから送信していた。これに対し、レイヤ2スイッチは、MACアドレステーブルから宛先ポートを検索できなかった(エントリがヒットしなかった)場合には、当該フレームを、レイヤ2スイッチが属するサブネット内に同報送信(ブロードキャスト)していた。

また、従来においても、MACアドレステーブルのエントリに対し、上述したようなエージング処理が行われていた。

このような従来のレイヤ2スイッチに対して、フレーム中継装置10は、MACアドレステーブル12を用いて、以下のレイヤ2中継処理を行う。

図4は、レイヤ2中継処理部11によるレイヤ2中継処理を示すフローチャートの一例である。本処理が開始すると、最初に、レイヤ2中継処理部11は、受信したフレームの送信元MACアドレスを抽出する(S101)。

レイヤ2中継処理部11は、検索条件の一つとして、抽出した送信元MACアドレスを含むことを設定する。また、レイヤ2中継処理部11は、検索条件の一つとして、レイヤ2中継処理でIPアドレスを考慮しない条件(例えば、「don't care」)とする。そして、レイヤ2中継処理部11は、これらの検索条件に基づいて、MACアドレステーブル12から送信元MACアドレスと同じMACアドレスを含むエントリを検索する(S102)。

レイヤ2中継処理部11は、MACアドレステーブル12を検索した結果、検索対象のMACアドレスの情報(検索に引っかかるエントリ)があるか否かを判断する。そして、レイヤ2中継処理部11は、MACアドレスのエントリが検索された場合に、このフレームを受信したポート15がMACアドレステーブル12内のエントリの宛先ポートと一致しているか否かを判断する(S103)。

このとき、S103の処理において、いずれの条件も満たした場合(S103: Yes)には、レイヤ2中継処理部11は、S104の処理を行う。また、

S 1 0 3 の処理において、いずれかの条件が満たされない場合（S 1 0 3 : N o）は、中継対象のフレームではない（なりすましのフレーム）と判断して、本処理を終了する。S 1 0 3 にてN oと判断されたときのフレームは、フレーム中継装置 1 0 において、中継対象のフレームとして取り扱われない。例えば、当該フレームはフレーム中継装置 1 0 内で廃棄される。

S 1 0 3 の処理においていずれの条件も満たした場合には、レイヤ 2 中継処理部 1 1 は、受信されたフレームから、宛先MACアドレスを抽出する（S 1 0 4）。

レイヤ 2 中継処理部 1 1 は、抽出した宛先MACアドレスを、検索対象のMACアドレスとする（エントリの検索条件に設定する）。このとき、レイヤ 2 中継処理部 1 1 は、IPアドレスを「don't care」、即ちエントリの検索条件に含めない。そして、レイヤ 2 中継処理部 1 1 は、これらの検索条件に基づいて、MACアドレステーブル 1 2 から宛先MACアドレスを検索する（S 1 0 5）。

レイヤ 2 中継処理部 1 1 は、MACアドレステーブル 1 2 を検索した結果、検索対象の宛先MACアドレスが検索された（検索条件に合致するエントリが検索に引っかかった）場合には、このMACアドレスに対応する宛先ポート宛にフレームを送信する（S 1 0 6）。但し、検索対象の宛先MACアドレスが検索されなかった（エントリにヒットしなかった）場合には、フレーム中継装置 1 0 に接続するサブネット内（受信ポートを除く他のポート）に同報送信する。

上述したレイヤ 2 中継処理によれば、図 4 に示すように、従来における中継処理（図 2）に S 1 0 3 の判断処理が付加され、この判断処理においてMACアドレスとポートとの対応関係がMACアドレステーブル 1 2 の登録内容に合致しなければ、当該フレームがなりすましのフレームであるものとして当該中継処理を終了する。これによって、なりすましのフレームの中継処理を防止することができる。

〈レイヤ 2 アドレス学習処理〉

次に、フレーム中継装置 1 0 で実行されるレイヤ 2 アドレス学習処理について説明する。このレイヤ 2 アドレス学習処理は、なりすましたフレームを中継対象のフレームとしてMACアドレステーブル 1 2 に登録されることを防止する。

図5は、本発明との比較のための、従来のレイヤ2スイッチにおけるレイヤ2アドレス学習処理を説明するフローチャートの一例である。レイヤ2アドレス学習処理とは、レイヤ2の中継処理を行う際に必要なMACアドレスを、MACアドレステーブルに追加または更新する処理である。

図5に示す例では、レイヤ2スイッチは、受信フレームから送信元MACアドレスを抽出し、当該MACアドレスを含むエントリがMACアドレステーブルに既に登録されているか否かを判定する。そして、該当するエントリがない場合、又は当該MACアドレスを含むエントリがあるがこのエントリ中の宛先ポートと当該受信フレームの受信ポートとが一致しない場合にMACアドレステーブル登録処理を行う。一方、レイヤ2スイッチは、当該フレームの送信元MACアドレス及び受信ポートがヒットしたエントリに合致する場合には、MACアドレステーブル登録処理を行わず、当該処理を終了する。

このような従来のレイヤ2スイッチのレイヤ2アドレス学習処理に対して、フレーム中継装置10のレイヤ2アドレス学習処理部13は、MACアドレステーブル12及び許容MACアドレステーブル14を用いて、以下のレイヤ2アドレス学習処理を行う。

図6は、レイヤ2アドレス学習処理部13による、レイヤ2アドレス学習処理の一例を説明するフローチャートである。

本処理が開始すると、最初に、レイヤ2アドレス学習処理部13は、許容MACアドレステーブル14を参照して、受信したフレームを受信したポート15の端末直結モードがオン(ON)であるか否かを判断する(S201)。

ここに、「端末直結モード」とは、端末がフレーム中継装置10の或るポートに直接に(他のHUBやスイッチを介さずに)接続されている場合に適用されるモードを指し、フレーム中継装置10のポート単位でそのオン/オフができるように構成される。端末直結モードがオンである場合には、レイヤ2アドレス学習処理部13は、許容MACアドレステーブル14を用いて登録可能なMACアドレスのチェックを行う。これに対し、端末直結モードがオフの場合には、レイヤ2アドレス学習処理部13は、登録可能なMACアドレスのチェックを行わない。

S201において、受信ポートの端末直結モードがONではない(OFFであ

る)と判断される場合 (S 2 0 1 : N o) には、レイヤ 2 アドレス学習処理部 1 3 は、S 2 0 6 の処理に移行する。これに対し、S 2 0 1 において、端末直結モードが ON であると判断される場合 (S 2 0 1 : Y e s) には、レイヤ 2 アドレス学習処理部 1 3 は、S 2 0 2 の処理に移行する。

端末直結モードが ON である場合に、レイヤ 2 アドレス学習処理部 1 3 は、フレームを受信したポート 1 5 のポート番号 (受信ポート番号) と同一のポート番号を含むエントリを、許容 MAC アドレステーブル 1 4 から取得する (S 2 0 2)。

フレーム中継装置 1 0 の起動直後では、許容 MAC アドレステーブル 1 4 の全てのエントリに対し、“無効” が設定されるように、フレーム中継装置 1 0 が構成される。この時点では、MAC アドレステーブル 1 2 には、登録エントリがないので、許容 MAC テーブル 1 4 で有効が設定された MAC アドレスに係るエントリのみが MAC アドレステーブル 1 2 に登録されるようにするためである。また、フレーム中継装置 1 0 (例えば、レイヤ 2 アドレス学習処理部 1 3) は、フレーム中継装置 1 0 が持つポート P a (a = 1, 2, 3 . . .) に接続されたリンクが切れたことを認識した場合には、許容 MAC アドレステーブル 1 4 のる当該ポート番号 P a に対する MAC アドレスの有効/無効の設定を“無効”とする。このようなリンク切れの監視及び無効設定に係る処理は、フレーム中継装置 1 0 の起動時において常時行われるように構成される。

レイヤ 2 アドレス学習処理部 1 3 は、許容 MAC アドレステーブル 1 4 から取得したエントリを参照して、当該エントリの有効/無効フィールドに“有効 (○)” が設定されている否かを判断する (S 2 0 3)。このとき、有効/無効フィールドに“有効” が設定されている場合 (S 2 0 3 : Y e s) には、レイヤ 2 アドレス学習処理部 1 3 は、S 2 0 5 の処理に移行する。これに対し、有効/無効フィールドに“有効” が設定されていない (“無効 (×)”) が設定されている場合 (S 2 0 3 : N o) には、レイヤ 2 アドレス学習処理部 1 3 は、S 2 0 4 の処理に移行する。

S 2 0 4 では、レイヤ 2 アドレス学習処理部 1 3 は、処理対象のフレームに係る情報を許容 MAC アドレステーブル 1 4 に登録する処理を行う。このとき、レイヤ 2 アドレス学習処理部 1 3 は、許容 MAC アドレステーブル 1 4 における、

当該フレームの受信ポート番号に対応するエントリについて、有効／無効フィールドに“有効(O)”を設定するとともに、当該フレームの送信元MACアドレスを登録する。S 2 0 4の処理が終了すると、レイヤ2アドレス学習処理部13は、S 2 0 6の処理に移行する。

一方、S 2 0 5では、レイヤ2アドレス学習処理部13は、フレームの送信元MACアドレスが、S 2 0 2で取得されたエントリのMACアドレスのフィールドに登録されているMACアドレスと同一であるか否かを判断する。このとき、レイヤ2アドレス学習処理部13は、MACアドレスが同一でない場合(S 2 0 5 : No)には、このフレームをなりすましのフレームであると判断して、本学習処理を終了する。これに対し、MACアドレスが同一である場合には、S 2 0 6の処理の処理に移行する。

S 2 0 6では、レイヤ2アドレス学習処理部13は、受信したフレームに係る情報をMACアドレステーブル12に登録する。このとき、レイヤ2アドレス学習処理部13は、このフレームに対応する情報として、テーブル12のMACアドレスのフィールドに対してフレームの送信元MACアドレスが設定され、IPアドレスのフィールドに対して“don't care”が設定され、宛先ポートのフィールドにフレームの受信ポート番号が設定され、ルーティング対象であるか否かの情報を格納するフィールドにルーティング対象でないことを示す情報(フラグ。

「O」及び「X」のような二値で表現できる。)が設定されたエントリをMACアドレステーブル12に登録する。S 2 0 6の処理が終了すると、レイヤ2アドレス学習処理部13は、本学習処理を終了する。

以上説明したフレーム中継装置10によると、次の作用効果を得ることができる。即ち、端末直結モードがオンにされるような、端末とフレーム中継装置10とが直接接続されている状況下では、その端末を収容するポートP aは、その端末のMACアドレスが送信元アドレスに設定されたフレームしか受信しない筈である。このため、当該ポートP aに対して有効なMACアドレスが許容MACアドレステーブル14に登録されている場合において、登録されたMACアドレスと異なる送信元MACアドレスを持つフレームが当該ポートP aから受信された場合には、当該端末がなりすましのフレームを送信した可能性が高い。フレーム

中継装置 10 の学習処理によれば、このようなフレームに対しては S 205 の判断で学習処理を途中で終了することで、当該フレームに係るエントリが MAC アドレス学習テーブル 12 に登録されることが防止される。また、フレーム中継装置 10 のフレームの中継処理によれば、当該フレームの中継処理が S 103 の判断で中止されるので、当該フレームが中継されることはない。

以上のように、フレーム中継装置 10 によれば、自装置と直結している端末からのなりすましのフレームの中継を防止することができる。従って、中継装置に対し複雑なフィルタリング設定を行う必要はない。また、なりすましのフレームがインターネットやイントラネット上に流れ込むのを抑えることができる。

なお、上述したレイヤ 2 アドレス学習処理において、端末直結モードが OFF の場合に許容 MAC アドレステーブル 14 によるチェック処理を行わない理由は次の通りである。

フレーム中継装置 10 に他のレイヤ 2 スイッチやスイッチング HUB がカスケード接続される場合では、フレーム中継装置 10 の他のレイヤ 2 スイッチを収容するポートには、他のレイヤ 2 スイッチの先に接続する複数の端末の MAC アドレスが、送信元 MAC アドレスとして到着する。この場合に、端末直結モードがオンであると、許容 MAC アドレステーブル 14 は、一つのポートに対して一つの MAC アドレスしか有効な MAC アドレスとして登録しないので、有効として登録された MAC アドレス以外の MAC アドレスの中継が行われなくなってしまう。このような状況を防止すべく、一つのポートに対して複数の正常な送信元 MAC アドレスを持つフレームが受信されるような接続状況下では、端末直結モードをオフにできるようにしている。

なお、上述したフレーム中継装置 10 の構成では、MAC アドレステーブル 12 に IP アドレス及びルーティング対象か否かを示す情報を登録するフィールドを設け、図 4 及び図 6 において、IP アドレスの検索や登録に係る処理を行う (S 102, S 105, S 206)。このようなレイヤ 3 に係る構成は、フレーム中継装置 10 に無くても良い。

〈第 2 の実施の形態〉

次に、本発明のフレーム中継装置の第 2 の実施の形態について説明する。

図7は、第2の実施の形態に係るフレーム中継装置20の構成を示すブロック図である。フレーム中継装置20は、MACアドレステーブル12、許容MACアドレステーブル14、レイヤ2中継処理部21（本発明のレイヤ2中継処理手段に対応）、スイッチ22、レイヤ2アドレス学習処理部23、中継対象識別部24、ポート25、ルーティング処理部（本発明のレイヤ3中継処理手段に対応）26、ルーティング対象登録処理部27、及びルーティング対象チェック部28を備える。

ルーティング対象登録処理部27は、本発明のフレーム中継装置における中継対象登録手段として機能する。また、ルーティング対象チェック部28は、本発明の判定手段として機能する。

なお、フレーム中継装置20の構成のうち、レイヤ2中継処理部21、レイヤ2アドレス学習処理部23、ポート25の構成は、第1の実施の形態におけるフレーム中継装置10のレイヤ2中継処理部11、レイヤ2アドレス学習処理部13、ポート15と同様である。従って、第2の実施の形態において、これらの機能に関する説明は省略する。

スイッチ22は、レイヤ2中継処理部21やルーティング処理部26で決定されたポートへ向けて、中継対象のフレームを転送する。スイッチ22は、従来の装置に搭載されているものを適用することができる。

中継対象識別部24は、複数（例えばn個）のポート25からそれぞれ受信される各フレームが、レイヤ2の中継対象であるかあるいはレイヤ3の中継対象であるかを、受信したフレームの宛先MACアドレスに基づいて判断する。なお、この中継対象識別部24の機能は、従来の装置の機能と同様の機能でもよい。

ルーティング対象チェック部28は、MACアドレステーブル12を参照して、受信したフレームに対する後述のルーティング前処理を実行する。ルーティング前処理後、ルーティング対象チェック部28は、受信したフレームがルーティング対象であるか否かによって、受信したフレームをルーティング処理部26またはルーティング対象登録処理部27に送信する。このルーティング対象チェック部28は、本発明に係る新規な構成である。

ルーティング処理部26は、ルーティング対象チェック部28から受信した、ルーティング対象のフレームに対するルーティング処理（レイヤ3の中継処理）

を行う。なお、このルーティング処理部 26 によるルーティング処理は、従来のルータによるルーティング処理と同様の処理でもよい。

ルーティング対象登録処理部 27 は、ルーティング対象チェック部 28 においてルーティング対象ではないと判定されたフレームに対して、後述のルーティング対象登録処理を行う。このルーティング対象登録処理部 27 は、本発明に係る新規な構成である。

〈ルーティング前処理〉

次に、本フレーム中継装置 20 のルーティング対象チェック部 28 による、ルーティング前処理について説明する。

図 8 は、本ルーティング対象チェック部 28 による、ルーティング前処理の一例について説明するフローチャートである。前処理が開始すると、最初に、ルーティング対象チェック部 28 は、受信したフレームの受信ポート番号に基づいて、このフレームに対するルーティング対象チェックを行うか否か（ルーティング対象チェックモードが ON か否か）を判断する（図 8 における S301）。

ここで、ルーティング対象チェックモードについて説明する。ルーティング対象チェックモードとは、受信フレームの送信元 MAC アドレスと送信元 IP アドレスの組から、当該受信フレームがフレーム中継装置 20 におけるルーティング対象であるか否かのチェックを実行するモードである。すなわち、ルーティング対象チェックモードを設定しない場合（チェックモード：OFF）には、受信したフレームに対してルーティング対象であるか否かのチェックを行わない。これに対し、ルーティング対象チェックモードが ON の場合には、受信フレームがルーティング対象か否かのチェックが行われる。ルーティング対象チェックモードは、各ポート番号単位にチェックを実行するか否か（モードの ON/OFF）を設定することができる。

S301 において、フレームの受信ポートに対するルーティング対象チェックモードが ON である場合（S301：Yes）には、ルーティング対象チェック部 28 は、S302 の処理に移行する。また、ルーティング対象チェックモードが OFF である場合（S301：No）には、ルーティング対象チェック部 28 は、ルーティング前処理を終了して、フレームをルーティング処理部 26 に送信する。そして、ルーティング処理部 26 によるフレームのルーティング処理が行われる。

なお、ルーティング処理は、従来と同様の処理であるので、説明は省略する。

ルーティング対象チェックモードがONである場合には、ルーティング対象チェック部28は、受信したフレームから送信元MACアドレス、及び送信元IPアドレスを抽出する(S302)。

送信元MACアドレス及び送信元IPアドレス抽出後、ルーティング対象チェック部28は、このMACアドレスとIPアドレスとの組み合わせを持つエントリを、MACアドレステーブル12から検索する(S303)。

ルーティング対象チェック部28は、S303で検索した結果、MACアドレステーブル12に対応する組み合わせ(エントリ)があるか否かを判断する。さらに、ルーティング対象チェック部28は、該当するエントリがある場合に、そのエントリがルーティング対象であるか否かを、検索されたエントリ中のルーティング対象か否かを示す情報(フラグ)に基づいて判断する(S304)。このとき、ルーティング対象チェック部28は、このエントリがMACアドレステーブル12から検索されない場合とこのフレームがルーティング対象ではない場合のいずれかである場合(S304: No)には、このフレームをルーティング対象登録処理部27に送信する。これにより、当該フレームについて、ルーティング対象登録処理部27によるルーティング対象登録処理が実行される。

また、ルーティング対象チェック部28は、受信したフレームが上記の条件のいずれも満たした場合(S304: Yes)には、このフレームをルーティング処理部26に送信する。

以上のような前処理によれば、MACアドレステーブル12において、ルーティング対象である旨が登録されたMACアドレス及びIPアドレスがそれぞれ送信元アドレスとして設定されたフレームのみが、ルーティング処理部26によるルーティング処理(中継処理)の対象となる。

〈ルーティング対象登録処理〉

次に、ルーティング対象登録処理部27による、ルーティング対象登録処理について説明する。

図9、10は、ルーティング対象登録処理部27による、ルーティング対象登録処理の一例を説明するフローチャートである。

まず、ルーティング対象登録処理部 27 は、ルーティング対象チェック部 28 から受信したフレームの受信ポートに対応する端末直結モードが ON であるか否かを判断する (S 401)。このとき、端末直結モードが ON である場合 (S 401 : Yes) には、ルーティング対象登録処理部 27 は S 402 の処理に移行する。また、端末直結モードが OFF である場合 (S 401 : No) には、ルーティング対象登録処理部 27 は、S 406 の処理に移行する。

端末直結モードが ON である場合には、ルーティング対象登録処理部 27 は、受信したフレームの受信ポート番号と同一のポートを持つエントリを、許容 MAC アドレステーブル 14 から取得する (S 402)。

続いて、ルーティング対象登録処理部 27 は、許容 MAC アドレステーブル 14 の情報に基づいて、このエントリに含まれる MAC アドレスの有効/無効を示す値を格納するフィールド(有効フィールド)の値が“有効”であるか否かを判断する (S 403)。このとき、有効フィールドの値が有効ではない場合 (S 403 : No) には、ルーティング対象登録処理部 27 は、このフレームの送信元 MAC アドレスに係るエントリを許容 MAC アドレステーブル 14 に登録する (S 404)。このとき、許容 MAC アドレステーブル 14 には、当該フレームの受信ポートのポート番号、に対応するエントリの有効フィールドに対し、有効を示す値を設定するとともに、当該エントリの MAC アドレスの格納フィールドに対し、当該フレームの送信元 MAC アドレスを登録する。登録後、ルーティング対象登録処理部 27 は、S 406 の処理に移行する。

S 403 の処理において、検索されたエントリの有効フィールドの値が有効であると判断された場合には、ルーティング対象登録処理部 27 は、フレームの送信元 MAC アドレスが当該エントリの MAC アドレスと同一であるか否かを判断する (S 405)。このとき、フレームの送信元 MAC アドレスとエントリの MAC アドレスとが同一ではない場合 (S 405 : No) には、ルーティング対象登録処理部 27 は、このフレームがなりすましのフレームであるものとして、ルーティング対象として登録せずに本処理を終了する。これに対し、フレームの送信元 MAC アドレスとエントリの MAC アドレスとが同一である場合 (S 405 : Yes) には、ルーティング対象登録処理部 27 は、S 406 の処理に移行する。

S 4 0 1, 4 0 4, 4 0 5 の処理後、ルーティング対象登録処理部 2 7 は、受信したフレームの送信元 I P アドレスと同一の I P アドレス持つエントリを、M A C アドレステーブル 1 2 から検索する (S 4 0 6)。

そして、ルーティング対象登録処理部 2 7 は、M A C アドレステーブル 1 2 にフレームの送信元 I P アドレスと同一の I P アドレスを持つエントリがあったか否かを判断する (S 4 0 7)。このとき、該当するエントリがあった場合 (S 4 0 7 : Y e s) には、ルーティング対象登録処理部 2 7 は、このフレームがなりすましのフレームであるものとして、ルーティング対象として登録せずに本処理を終了する。

S 4 0 7 において、該当するエントリが検索されなかった場合 (S 4 0 7 : Y e s) には、ルーティング対象登録処理部 2 7 は、当該フレームがなりすましのフレームか否かを判断するために、当該フレームの送信元 M A C アドレスを問い合わせ先の M A C アドレスとした A R P (Address Resolution Protocol) 要求フレームを送信する (S 4 0 8)。即ち、フレームに設定された送信元 I P アドレスに対応する M A C アドレスを問い合わせるための A R P 要求フレームを生成し、受信したフレームの送信元 M A C アドレス宛に送信する。

ルーティング対象登録処理部 2 7 は、A R P 要求フレームに対する応答が所定時間内にあり (所定時間内に A R P 応答フレームを受信し)、かつ応答フレームに入っている M A C アドレス (問い合わせ元の I P アドレスに対応する M A C アドレス) が、受信したフレームの送信元 M A C アドレスと同一であるか否かを判断する (S 4 0 9)。

応答フレームを所定期間内に受信しなかった場合、或いは応答フレーム中の M A C アドレスとフレームの送信元 M A C アドレスとが一致しなかった場合 (S 4 0 9 : N o) には、ルーティング対象登録処理部 2 7 は、受信したフレームがなりすましのフレームであるものとして、このフレームをルーティング対象として登録せずに本処理を終了する。

S 4 0 8 において、A R P 要求フレームの代わりに ping (Packet INternet Groper) フレームを送信するようにしても良い。この場合には、ping フレームの宛先 M A C アドレスには、当該フレームの送信元 M A C アドレスを設定し、且

つ宛先IPアドレスには、当該フレームの送信元IPアドレスを設定する。

ping フレームを送信する場合には、ルーティング対象登録処理部27は、S409において、ping の Reply フレームを所定期間内に受信でき、この ping の Reply フレームの送信元MACアドレスと送信元IPアドレスとが、受信したフレームの送信元MACアドレスと送信元MACアドレスと一致するか否かを判断する。Reply フレームを所定期間内に受信できなかった場合、及び Reply フレームの送信元MACアドレス及び送信元IPアドレスがフレームの送信元MACアドレス及び送信元IPアドレスに一致しない場合 (S409: No) には、処理を終了し、そうでない場合 (S409: Yes) には、処理をS410に進める。

S409において、所定期間内に受信された応答フレーム中の問い合わせ先のMACアドレスがフレームの送信元MACアドレスに一致する場合、即ち、問い合わせに対する正常な応答が得られた場合には、ルーティング対象登録処理部27は、受信したフレームの送信元MACアドレスと同一のMACアドレスを持ち、かつIPアドレスに対する設定が「don't care」であるエントリがMACアドレステーブル12に存在するか否かを判断する (S410)。

S410において、上記条件を満たすエントリがMACアドレステーブル12に存在する (該当するエントリが見つかった) 場合 (S410: Yes) には、ルーティング対象登録処理部27は、当該エントリの内容を、以下のように書き換える (更新する)。すなわち、ルーティング対象登録処理部27は、当該エントリのMACアドレスのフィールドに対してフレームの送信元MACアドレスを登録し、IPアドレスのフィールドに対してフレームの送信元IPアドレスを登録し、宛先ポート番号のフィールドに対してフレームの受信ポート番号を登録し、ルーティング対象か否かを示す情報を格納するフィールドにルーティング対象であることを示す値 (フラグ値)、例えば0) を登録する (S411)。S411が終了すると、ルーティング対象登録処理部27は、本処理を終了する。

S410において、条件を満たすエントリがMACアドレステーブル12に存在しない場合には、ルーティング対象登録処理部27は、受信したフレームの送信元MACアドレスと同一のMACアドレスを持つ、MACアドレステーブル12のエントリの数を取得する (S412)。

そして、取得したエントリの数、が、予め定められた同一のMACアドレスに対するIPアドレスの登録可能数未満であるか否かを判断する（S413）。ここで、同一のMACアドレスに対するIPアドレスの登録可能数について説明する。IPアドレスの登録可能数とは、MACアドレステーブル12に対し、同一のMACアドレスに対応する異なるIPアドレスの登録（MACアドレスが同一でIPアドレスが異なるエントリの登録）を幾つまで許容するかを指定する値である。例えば、IPアドレスの登録可能数として、2を設定した場合は、あるMACアドレスが共通でIPアドレスが異なるエントリを2つまでMACアドレステーブル12に登録することができることを示す。なお、IPアドレスの登録可能数は、ルーティング対象登録処理部27がアクセス可能なメモリ（図示せず）上に予め用意される。当該登録可能数は、ユーザインターフェイス等を介して変更可能に構成することができる。

S413において、取得したエントリの数、がIPアドレスの登録可能数未満である場合には、ルーティング対象登録処理部27は、MACアドレステーブル12に対し、当該フレームに係るエントリを登録する。具体的には、エントリのMACアドレスのフィールドにフレームの送信元MACアドレスが設定されIPアドレスのフィールドにフレームの送信元IPアドレスが設定され、宛先ポート番号のフィールドにフレームの受信ポート番号が設定され、ルーティング対象か否かを示す値の格納フィールドにルーティング対象であることを示す値が設定されたエントリを、MACアドレステーブル12に登録する（S414）。そして、MACアドレステーブル12への書き込み終了後、ルーティング対象登録処理部27は本処理を終了する。

S413において、取得したエントリの数、がIPアドレスの登録可能数以上である場合（S413：No）には、このエントリに対してはこれ以上IPアドレスの登録は不可能、すなわち、このフレームがなりすましである可能性があるとして登録せずに本処理を終了する。

上記のS414においてMACアドレステーブルに追加されるエントリは、上述した前処理やレイヤ2中継処理時において、最優先で検索（ヒット）される状態で、或いは、追加エントリと同一のMACアドレスを含む既登録の他のエントリよりも

先に検索（参照）される状態で登録される。この理由は、次の通りである。通常、送信元MACアドレスに対応する送信元IPアドレスは1つであるので、一つのMACアドレスについては一つのエントリ（一つのIPアドレス）のみがMACアドレステーブル12に登録されるようにすれば、その後、IPアドレスをなりすました（IPアドレスが異なる）フレームに対するエントリの登録を防止することができる。一方、端末が使用するIPアドレスが設定等により適正に変更されることは全く考えられない訳ではない。このため、IPアドレスの登録可能数を2以上に設定可能にすることで、MACアドレスが共通でIPアドレスが異なる複数のエントリがMACアドレステーブル12に登録されることを許容している。但し、端末が使用するIPアドレスは通常一つであるので、IPアドレスが変更された場合には、変更前のIPアドレスは使われなくなる。一方、上述したように、一定時間使用されなかったエントリは、エージング処理によって、MACアドレステーブル12から削除される。従って、上述したように、追加エントリが変更前のIPアドレスを含む他のエントリよりも先にヒットするように登録すれば、当該他のエントリをエージング処理によって自動的に削除することが可能となる。

なお、上述したS413の処理では、登録可能数未満か否かを判定しているが、登録可能数以下か否かで判定するようにしても良い。すなわち、登録可能数よりも多くの共通のMACアドレスを含むエントリがMACアドレステーブル12に登録されないようになっていれば良い。

また、ルーティング対象登録処理において、端末直結モードがONの時のみ許容MACアドレステーブルのチェックを行う理由は、該当ポートに端末でなくレイヤ2スイッチ等がカスケード接続されている場合に対応するためである。これは、第1の実施の形態で説明したのと同様の理由である。

〈実施の形態の効果〉

以上の本発明のフレーム中継装置に係る第1の実施の形態及び第2の実施の形態によれば、以下のような効果が得られる。

図5から、端末直結モードがONの時は、許容MACアドレステーブルで許可されたMACアドレスしか学習対象とならない。フレーム中継装置10又は20に直接繋がった端末が、MACアドレスのなりすましを行った場合、いままで通信して

きたMACアドレスで既に許容MACアドレステーブル14に対する登録が行われていることから、なりすましたMACアドレスでは学習処理が行われない。すなわちMACアドレステーブルにエントリが登録されないため、図4の中継方式で示したように、なりすましたMACアドレスは中継されないといった効果を得ることができる。

また、許容MACアドレステーブル14は、リンクが切れたときにそのリンクを収容するポートに対する有効/無効の設定が無効となる。このため、例えば別の端末に接続を変更した時は、許容MACアドレステーブル14の当該ポートに対するエントリのMACアドレスの有効/無効が無効となっているので、端末が通信を開始した時点でのMACアドレスで再登録がなされる。従って、フレーム中継装置10及び20によれば、ユーザが或るポートに対する端末の入れ替えや移動（ポートの変更）を行っても、アドレスのなりすましに対応することができる。

また、例えば、フレーム中継装置10及び20において、接続する他のレイヤ2スイッチの先にいる複数の端末のMACアドレスが送信元MACアドレスとして到着する場合、端末直結モードをONにすると、許容MACアドレステーブルのチェック処理によって、レイヤ2スイッチ配下の端末のうち1つだけしか通信できなくなってしまう。そのため、本フレーム中継装置10及びフレーム中継装置20では、端末直結モードをOFFに設定し、そのポートからのMACアドレスを全てMACアドレステーブルに登録できるようにすることで、全端末からの通信を確保することが可能となる。

〈変形例〉

本実施の形態に係るフレーム中継装置10及び20は、例えば以下のような変形や運用が可能である。

例えば、フレーム中継装置10又は20に対して他のレイヤ2スイッチ等がカスケード接続される場合には、端末直結モードをOFFにしなければならない。しかしながら、この場合には、許容MACアドレステーブル14を用いたMACアドレスのチェックが行われない。そこで、他のレイヤ2スイッチが接続されたポートからやってくるMACアドレスのなりすましフレームを防ぐために、他のレイヤ2スイッチをフレーム中継装置10に置き換え、そのフレーム中継装置10に端末が直

結されるように接続することで、そのフレーム中継装置 10 においてなりすましのフレーム中継を防止することができる。

また、フレーム中継装置 20 では、ルーティング対象チェックモードが ON の時のみルーティング対象のチェックを行っている。この理由は、該当ポート 25 に他のレイヤ 3 の中継装置（ルータやレイヤ 3 スイッチなど）が接続されている場合に対応するためである。フレーム中継装置 20 に他のレイヤ 3 の中継装置が接続されている場合には、当該他の中継装置から来るフレーム（ルーティングフレーム）の MAC アドレスは、全て他の中継装置の持つ MAC アドレスとなる。このため、フレーム中継装置 20 は、同一の送信元 MAC アドレスに対して多数の送信元 IP アドレスを受信する。すなわち、同一の送信元 MAC アドレスに対して送信元 IP アドレスが多数ある場合には、フレーム中継装置 20 ではなりすましと判断され、ルーティング対象とならない。この場合は、そのポート 25 に対するルーティング対象チェックモードを OFF にすることで、ルータ間接続にも対応することが可能となる。

但し、フレーム中継装置 20 において、ルーティング対象チェックモードを OFF にした場合、IP アドレスや MAC アドレスのなりすましを防ぐことはできない。その場合は、接続先のレイヤ 3 の中継装置をフレーム中継装置 20 に置き換える。このような置き換えによって、置き換えられたフレーム中継装置 20 において、なりすましのフレーム中継を防止することができる。

また、フレーム中継装置 20 では、ルーティング対象か否かの判断に用いるテーブルとして、従来の MAC アドレステーブルに改変を加えたテーブルを利用している。これによって、装置構成を簡易にするとともに、中継装置が従来持つエージング機能を用いて不要なエントリを削除することが可能となる。但し、MAC アドレステーブルとは別にルーティングの許可／不許可（対象か否か）を判断するための情報を登録するテーブルを別途もってもよい。ただし、その場合は、古いエントリの自動削除機能がなくなる（MAC アドレステーブルに融合させていることで、レイヤ 2 のエージング処理による自動削除を実現していたため）。このため、別途作成したテーブルにおいて、MAC アドレステーブルとは別にエージング処理を追加する必要がある。なお、この場合におけるエージング処理方法は、レイヤ 2 中継

処理でのエージング処理と同一の処理でよい。

また、MACアドレス／IPアドレスの双方をなりすまし、かつARPやpingに対する擬似応答まで行われる場合を防ぐには、フレーム中継装置20で、図4及び図5に示したような処理がルーティング対象登録処理とともに実行されるようにすれば良い。このようにすれば、MACアドレス／IPアドレスの双方をなりすましたフレームの中継も完全に防ぐことが可能となる。

さらに、フレーム中継装置20は、IPがIPv4である場合を想定して説明している。但し、IPがIPv6の場合でも処理を変更することなく対処が可能である。具体的には、IPv6を適用する場合には、MACアドレステーブルのIPアドレスの格納フィールドのサイズを、IPv4に応じた32ビットからIPv6に応じた128ビットに拡張する。また、図10のS408において、MACアドレスのチェックのために送信するフレームとして、ARPフレームの代わりにICMPv6の近隣要請メッセージを送信する。そして、ARP応答フレームの代わりにICMPv6の近隣通知メッセージを待ち受けるようにすれば良い。この場合、S409の判断処理に変更はない。このように、本発明に係るフレーム中継装置は、IPv4だけではなくIPv6にも対応することができる。

産業上の利用可能性

本発明は、アドレスのなりすましを防止するフレームの中継処理を提供する産業に適用可能である。

請求の範囲

1. 自装置でのフレームの中継処理で使用するMACアドレスとIPアドレスとの組を含むエントリが登録されるテーブルと、

受信されたフレーム中の送信元MACアドレス及び送信元IPアドレスで前記テーブルを検索し、この送信元アドレスの組がレイヤ3での中継対象として登録されているか否かを判定する判定手段と、

前記送信元アドレスの組が中継対象として登録されていると判定されたフレームのみを対象としてレイヤ3の中継処理を行うレイヤ3中継処理手段と、を含むフレーム中継装置。

2. 前記フレームの送信元アドレスの組が前記テーブルに登録されていなかった場合に、この送信元アドレスの組が正常か否かを問い合わせるための問い合わせフレームを送信し、この問い合わせフレームに対する応答フレームが前記問い合わせフレームを送信してから所定期間内に到着し且つこの応答フレーム中の情報が前記送信元アドレスの組が正常であることを示すという条件を満たすか否かを判定し、前記条件を満たす送信元アドレスの組を含むエントリを前記テーブルに登録し、前記条件を満たさない送信元アドレスの組を前記テーブルへの登録対象から除外する中継対象登録手段をさらに含む

請求項1記載のフレーム中継装置。

3. 前記中継対象登録手段は、前記問い合わせフレームとして前記フレームの送信元IPアドレスに対応するMACアドレスを問い合わせるためのARP要求フレームを送信し、前記応答フレームとしてARP応答フレームを受信し、このARP応答フレーム中の問い合わせ先のMACアドレスが前記フレームの送信元MACアドレスと一致する場合に、前記送信元アドレスの組み合わせが正常であると判定する

請求項2記載のフレーム中継装置。

4. 前記中継対象登録手段は、前記問い合わせフレームとして前記フレームの送信元MACアドレス及び送信元IPアドレスをそれぞれ宛先MACアドレス及び宛先IPアドレスとするpingフレームを送信し、前記応答フレームとして

ping リプライフレームを受信し、この ping リプライフレームの送信元MACアドレス及び送信元IPアドレスが前記フレームの送信元MACアドレス及び送信元IPアドレスにそれぞれ一致する場合に、前記送信元アドレスの組み合わせが正常であると判定する

請求項2記載のフレーム中継装置。

5. 前記中継対象登録手段は、前記フレームの送信元IPアドレスと同一のIPアドレスを含むエントリが既に前記テーブルに登録されている場合には、前記応答フレームに係る条件が満されるか否かに拘わらず、前記フレームの送信元アドレスの組を前記テーブルへの登録対象から除外する

請求項2～4の何れかに記載のフレーム中継装置。

6. 前記中継対象登録手段は、前記フレームの送信元MACアドレスと同一のMACアドレスを含むエントリが既に前記テーブルに登録されている場合には、前記応答フレームに係る条件が満されるか否かに拘わらず、前記フレームの送信元アドレスの組を前記テーブルへの登録対象から除外する

請求項2～5の何れかに記載のフレーム中継装置。

7. 前記テーブルに対してMACアドレスが同一でありIPアドレスが異なるエントリを登録可能な数が予め規定されており、

前記中継対象登録手段は、前記フレームの送信元MACアドレスと同一のMACアドレスを含む前記登録可能数以上のエントリが既に前記テーブルに登録されているときには、前記応答フレームに係る条件が満されるか否かに拘わらず、前記フレームの送信元アドレスの組を前記テーブルへの登録対象から除外する

請求項2～6の何れかに記載のフレーム中継装置。

8. 前記テーブルは、MACアドレスとこのMACアドレスに対応する宛先ポート番号とを含むエントリを格納し、フレームのレイヤ2での中継において宛先ポートを割り出すために参照されるMACアドレステーブルの各エントリに、MACアドレスに対応するIPアドレスのフィールドと、中継対象か否かを示す情報を格納するフィールドとを設けることによって構成され、

自装置で受信されるフレームのレイヤ2の中継処理を前記テーブルを参照して行うレイヤ2中継処理手段と、

前記テーブルから一定時間使用されなかったエントリを削除する削除手段とをさらに含む

請求項 1 ～ 7 の何れかに記載のフレーム中継装置。

9. 前記フレームの送信元アドレスの組を含むエントリを前記テーブルに登録する際に、この送信元アドレスの組を構成するMACアドレスと同一のMACアドレスを含む他のエントリが既に前記テーブルに登録されている場合には、前記判定手段による処理において当該エントリが前記他のエントリよりも先に検索される状態で当該エントリに登録する

請求項 8 記載のフレーム中継装置。

10. 自装置が有するポート毎に前記判定手段及び前記中継対象登録手段による処理を行うか否かを設定可能に構成されている

請求項 1 ～ 9 の何れかに記載のフレーム中継装置。

11. 自装置が有するポート毎に受信可能なMACアドレスを一つだけ登録可能なテーブルと、

各ポートで受信されたフレームに対し、このフレームの送信元MACアドレス及び受信ポート番号の組と同一のMACアドレス及びポート番号の組が前記テーブルに登録されているか否かを判定する判定手段と、

前記送信元MACアドレス及び受信ポート番号の組が登録されていると判定されたフレームのみを対象としてレイヤ 2 の中継処理を行う中継手段とを含むフレーム中継装置。

12. 前記フレームの送信元MACアドレスが、前記テーブルに登録されていない場合に、この送信元MACアドレス及び受信ポート番号の組が有効であるか否かを判定し、有効な送信元MACアドレス及び受信ポート番号の組を前記テーブルに登録する、MACアドレス学習部をさらに含む、請求項 11 に記載のフレーム中継装置。

13. 前記MACアドレス学習部は、前記ポートがフレームを受信可能な状態となってから、最初に受信したフレームの送信元MACアドレス及び受信ポート番号の組を、前記有効な組としてテーブルに登録する、請求項 12 に記載のフレーム中継装置。

14. 前記MACアドレス学習部は、送信元MACアドレス及び受信ポート番号の組が有効であるか否かの判断を行うか否かを個々のポート番号毎に設定可能である、請求項11または12に記載のフレーム中継装置。

15. 自装置が有するポート毎に受信可能なMACアドレスを一つだけ登録可能なテーブルと、

各ポートで受信されたフレームに対し、このフレームの送信元MACアドレス及び受信ポート番号の組と同一のMACアドレス及びポート番号の組が前記テーブルに登録されているか否かを判定する判定手段と、

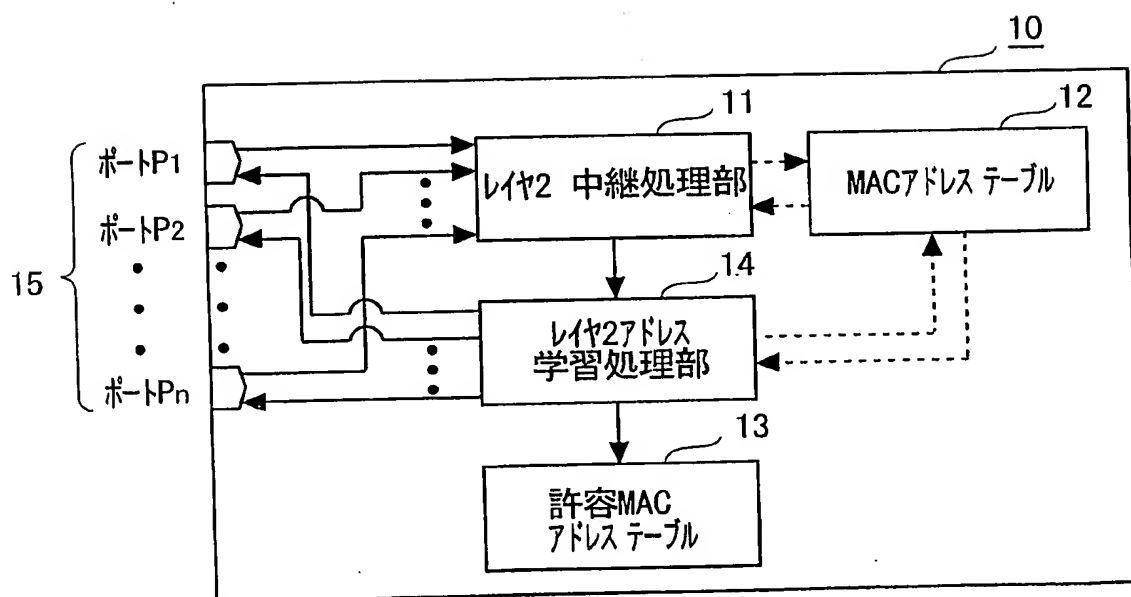
を含むフレーム判定装置。

16. 自装置でのフレームの中継処理で使用するMACアドレスとIPアドレスとの組を含むエントリが登録されるテーブルと、

受信されたフレーム中の送信元MACアドレス及び送信元IPアドレスで前記テーブルを検索し、この送信元アドレスの組がレイヤ3での中継対象として登録されているか否かを判定する判定手段とを含むフレーム判定装置。

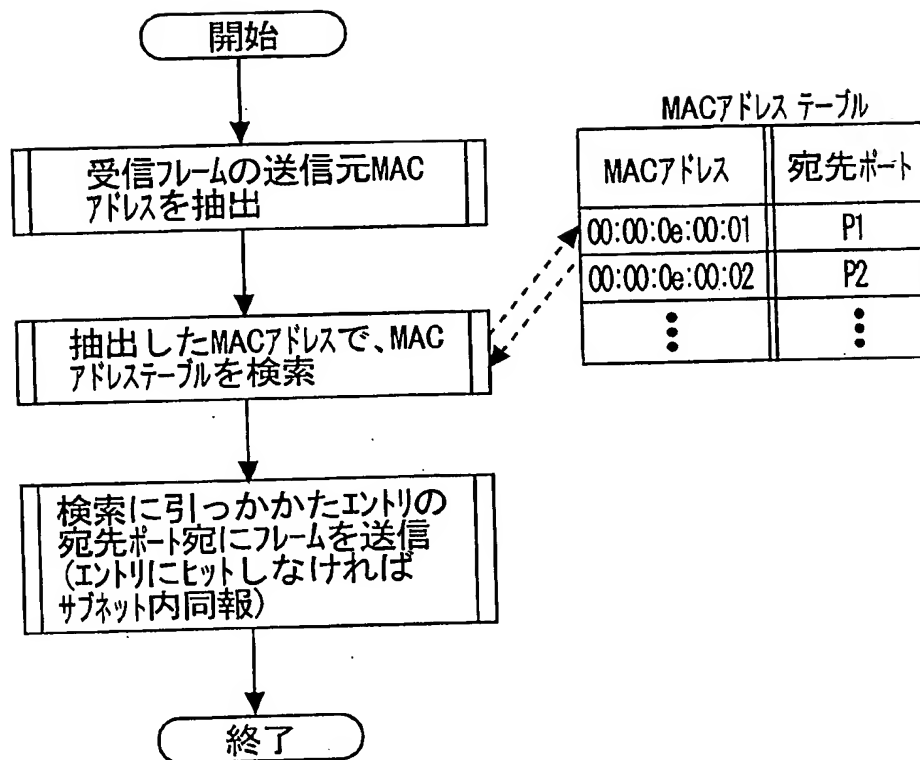
1/10

FIG. 1



2/10

FIG. 2



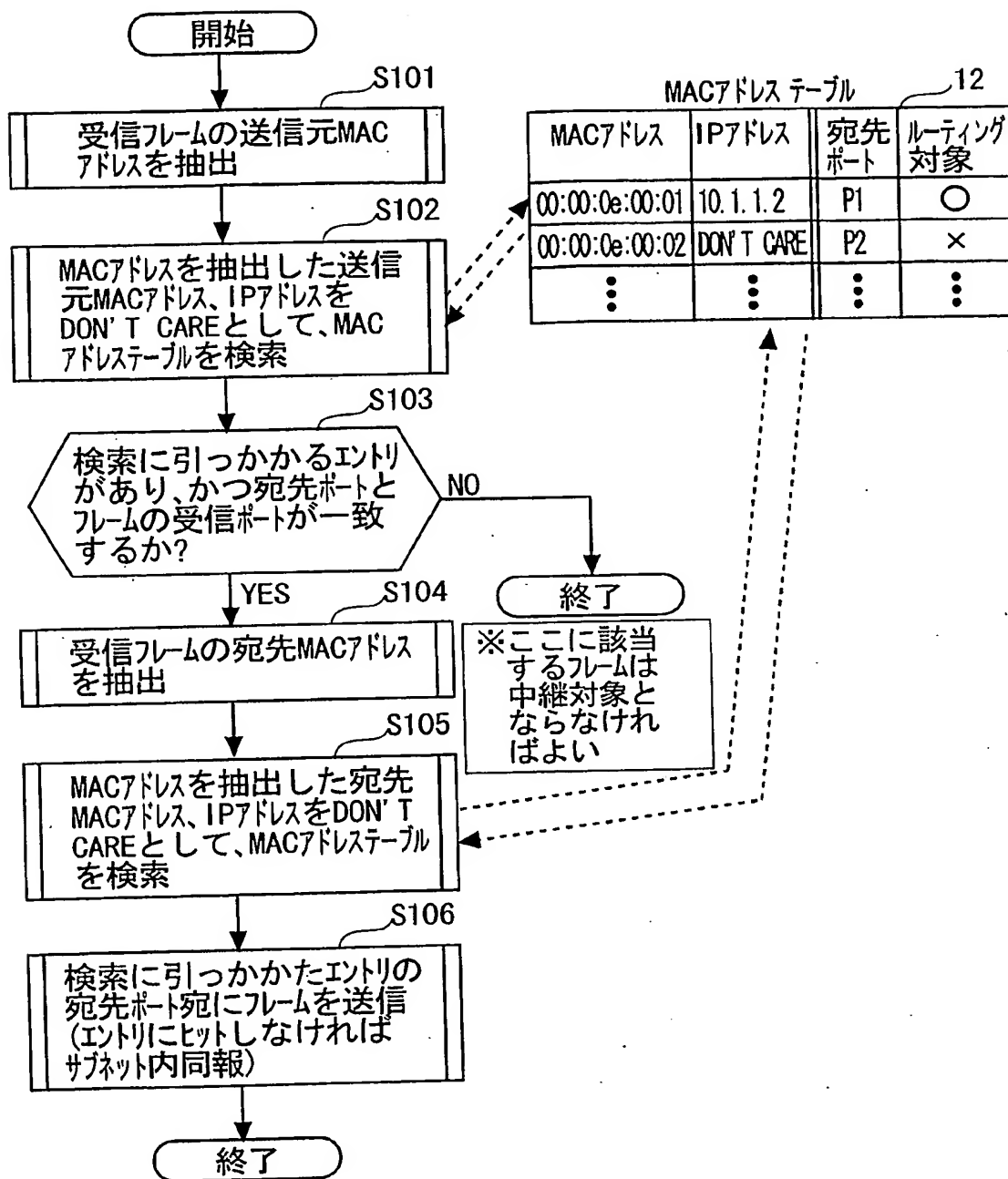
3/10

FIG. 3

MACアドレス テーブル

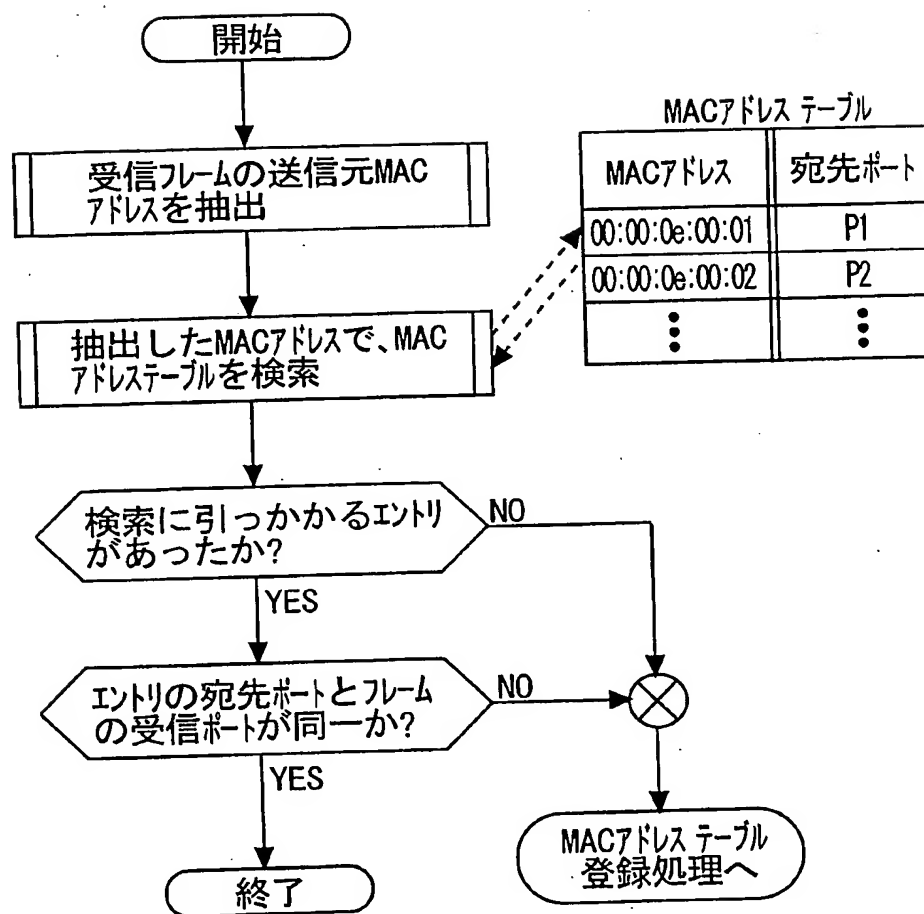
12

MACアドレス	IPアドレス	宛先ポート	ルーティング対象
00:00:0e:00:01	10. 1. 1. 2	P1	○
00:00:0e:00:02	DON' T CARE	P2	×
⋮	⋮	⋮	⋮

4/10
FIG. 4

5/10

FIG. 5



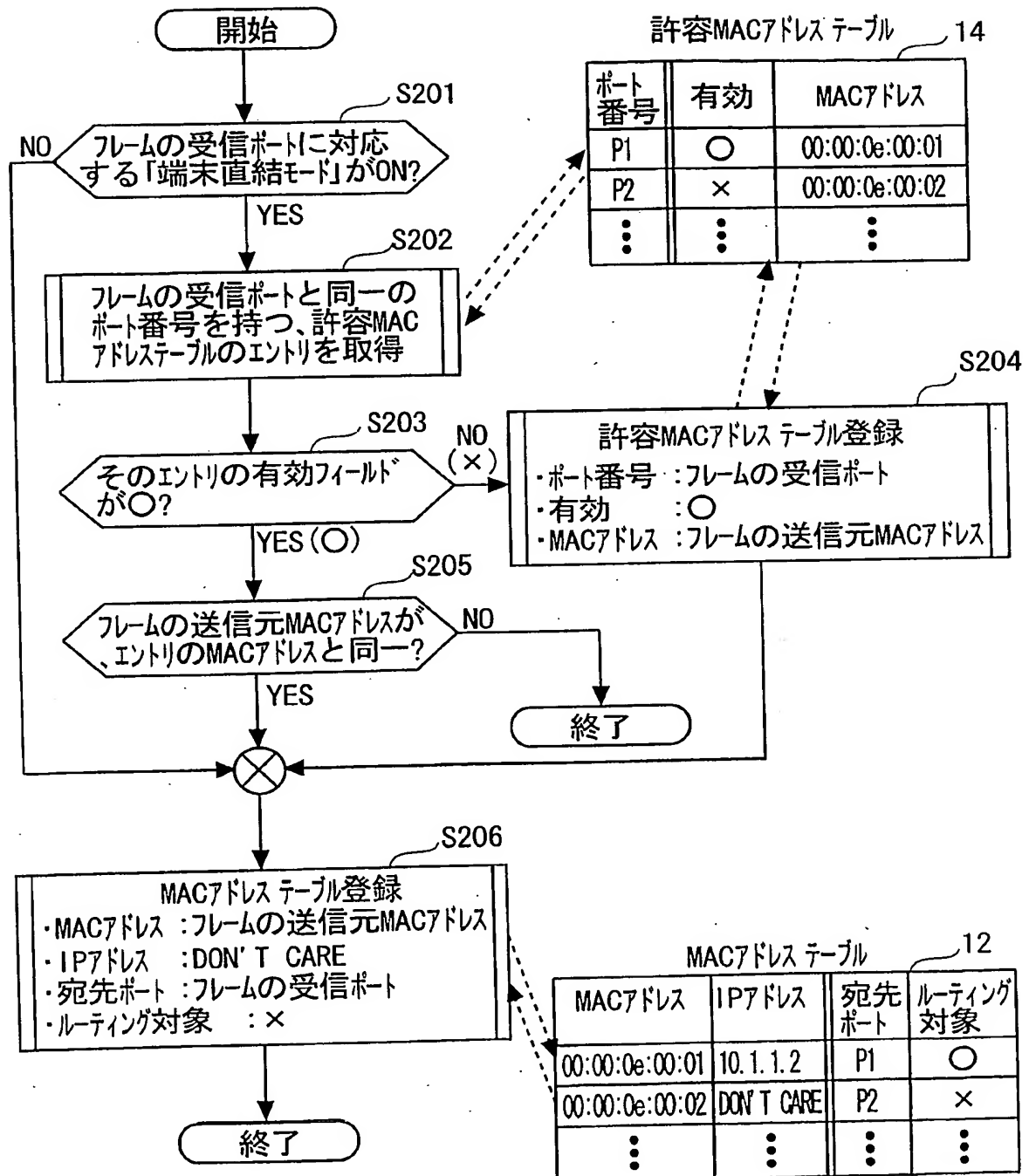
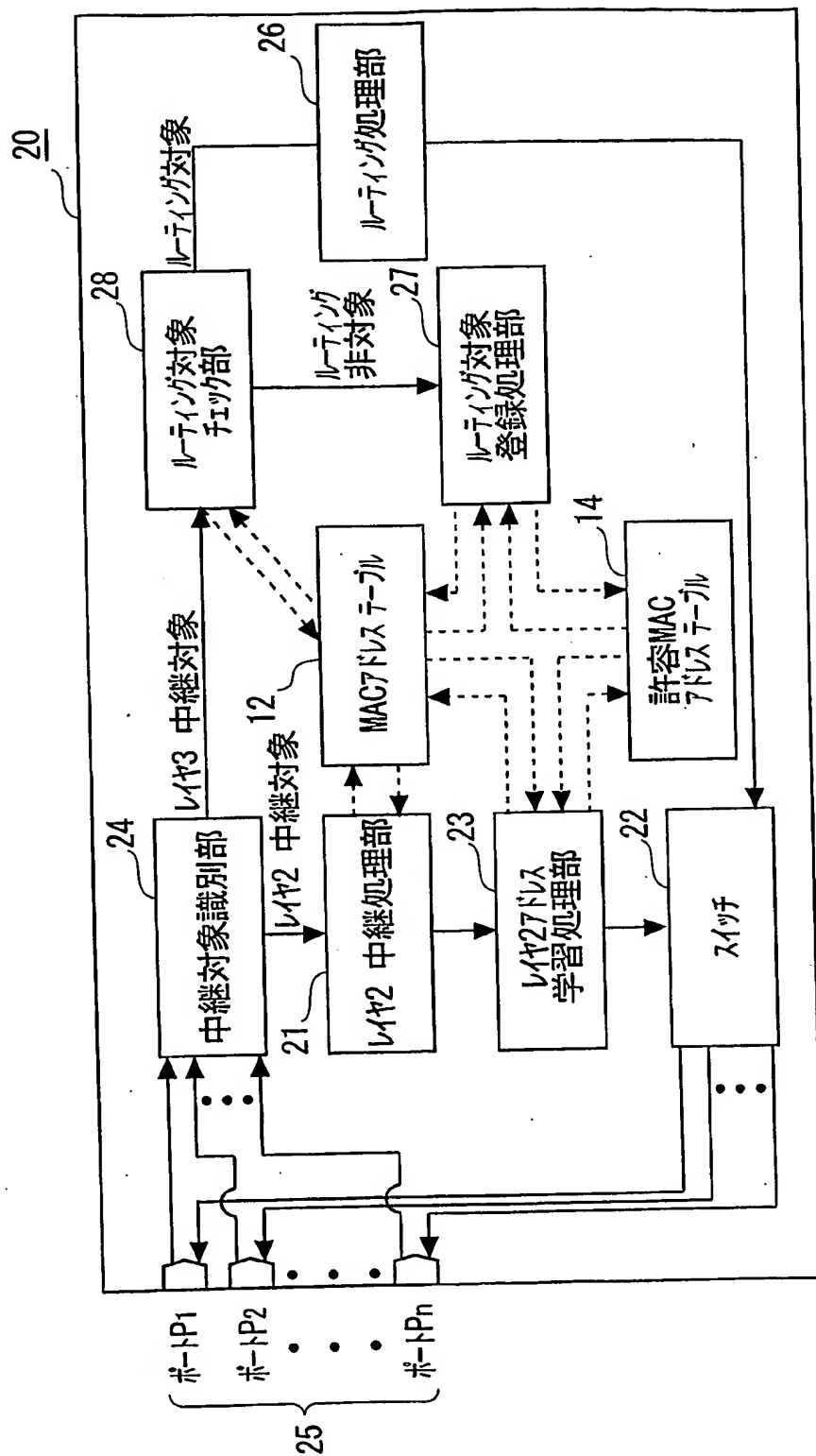
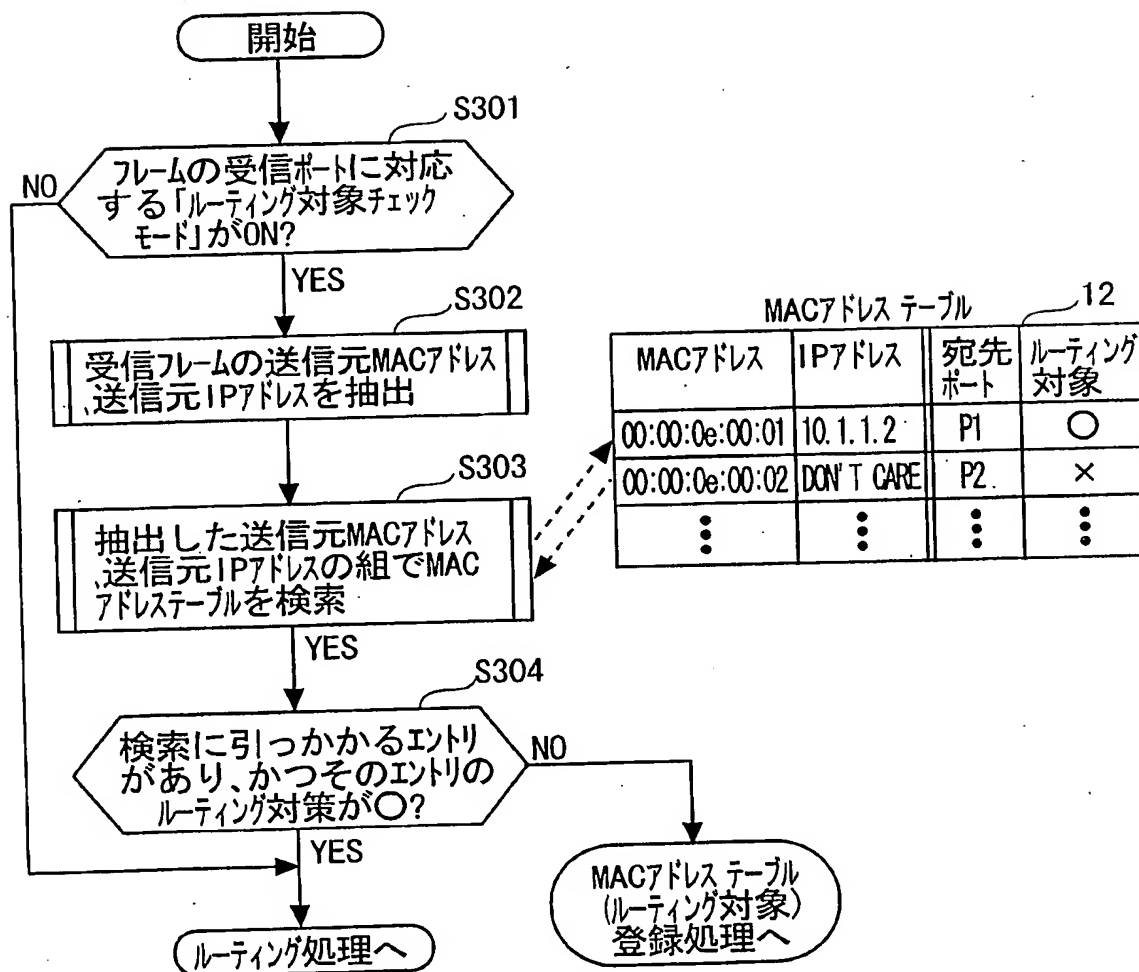
6/10
FIG. 6

FIG. 7



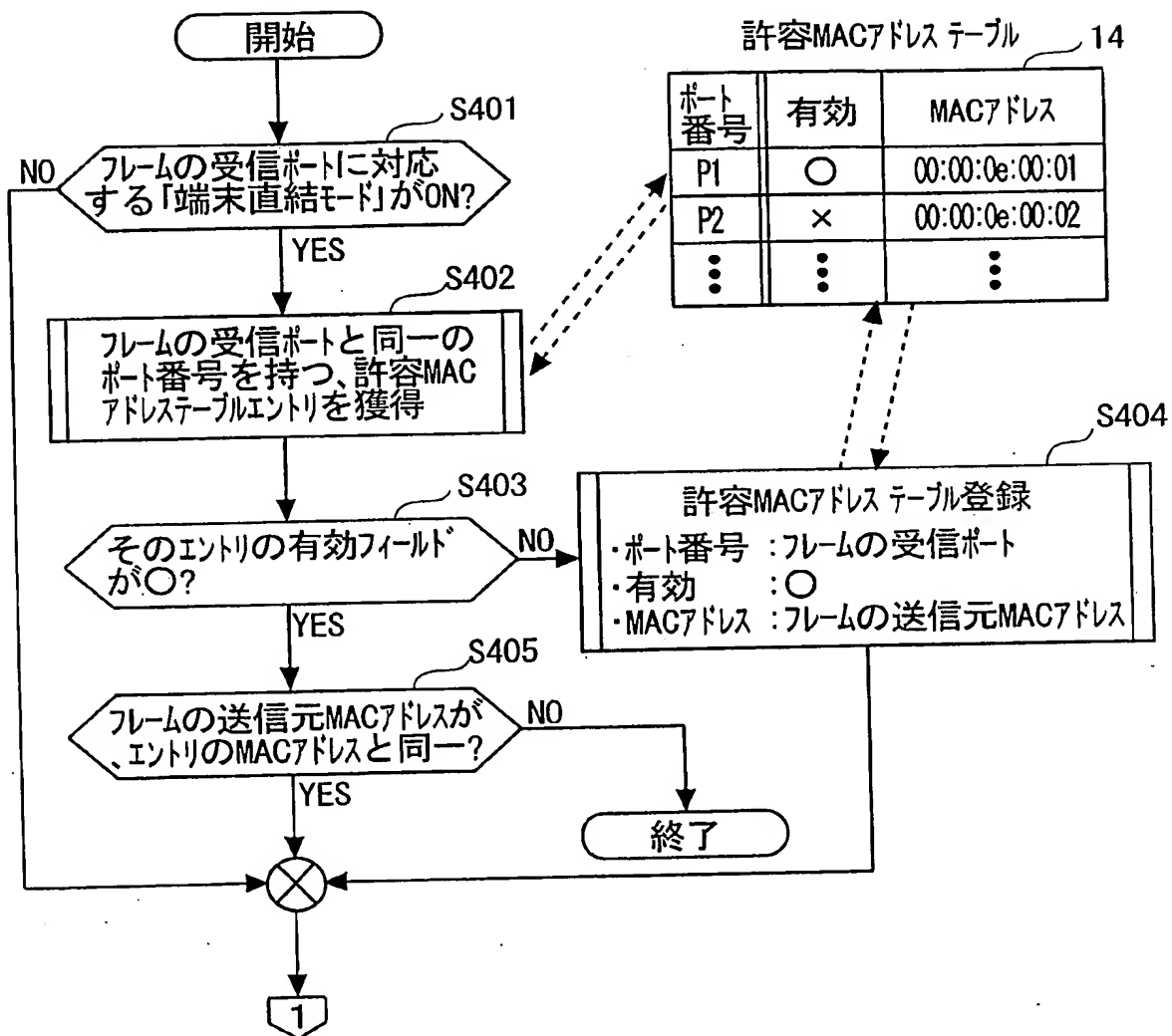
8/10

FIG. 8



9/10

FIG. 9



10/10

FIG. 10

